مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in SUSE NeuVector

Tracking #:432317849

Date:23-10-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in SUSE NeuVector. This flaw allows remote command injection and potential buffer overflow within the Enforcer container, leading to full compromise of protected container environments.

TECHNICAL DETAILS:

A critical security vulnerability has been identified in SUSE NeuVector, a container security and compliance platform widely used in Kubernetes and DevSecOps environments. Tracked as CVE-2025-54469, the flaw enables remote command injection and potential buffer overflow within the NeuVector Enforcer container, resulting in complete compromise of containerized environments.

Vulnerability Details

- **CVE-2025-54469**
- CVSS Score: 10.0 Critical
- The vulnerability exists in the Enforcer container's monitor process, responsible for managing subprocesses such as the Consul service. When the Enforcer container stops, the monitor uses the popen() function to execute a shell command that checks the Consul process status.
- Two environment variables, CLUSTER_RPC_PORT and CLUSTER_LAN_PORT, are used without sanitization or validation when constructing the shell command. This lack of input validation allows attackers to inject arbitrary commands, enabling execution of unauthorized code within the Enforcer container.
- Successful exploitation could allow attackers to:
    - Remote code execution with root privileges inside the Enforcer container.
    - Complete compromise of the containerized runtime environment.
    - Lateral movement across the Kubernetes cluster.
    - Tampering with NeuVector's runtime security enforcement mechanism.
    - Privilege escalation if the Enforcer container is executed with elevated permissions.

Affected Versions

- NeuVector >=5.3.0, <=5.4.6

Fixed Versions

- NeuVector 5.4.7, 5.3.5

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by SUSE.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://github.com/neuvector/neuvector/security/advisories/GHSA-c8g6-qrwh-m3vp